The future rôle of risk assessment in nuclear safety

by R. Niehaus*

The past decade has seen a growing number of scientific publications [1] and conferences on risk assessment. In some countries professional societies for risk analysis have been founded. Risk assessment studies have been performed on such diverse problems as acid rain, climatic change, the ozone layer, medical X-rays, new drugs, and so on. Other studies have analysed the perception of risk by the public. So-called Probabilistic Risk Analyses are being conducted for nuclear installations, chemical plants, liquified natural gas (LNG) terminals, etc. Recently, the United States Nuclear Regulatory Commission (US NRC) has decided to adopt qualitative safety goals supported by quantitative design objectives for nuclear plants for use during a two-year evaluation period [2]; compliance can only be proved by performing a risk analysis for normal operation and possible accidents. Given the rapid expansion of risk assessment on many fronts, one may ask whether risk assessment really offers something new as a scientific response to new demands created by technology, or whether it is only a short-term fad, something old in a new guise which will soon disappear. This question is even more justifiable in view of the fact that things were quite safe before risk assessment techniques were developed and applied.

This paper will explore:

- to what extent risk assessment offers new ways of increasing safety;
- the status of available tools; and
- promising areas for future applications.

Risk assessment denotes the total process of improving safety, and comprises three principal elements: *risk estimation,* the identification and quantification of risk; *risk evaluation,* the process of weighting and comparing different aspects of a risk; and *risk management,* the formulation and implementation of safety policy.

At present, safety is assured mainly by the use of deterministic criteria. An engineer designing a bridge will add a safety factor to his original design. Certain beams will for example be made twice as strong as would be required by pure mechanics with no safety margin. It is then assumed that the safety factor will compensate for undetected deficiencies in steel quality, welding, construction etc., and for some unpredictable events. Of course, foreseeable events such as high-water level or wind speed, or earthquakes, will also be considered. Appropriate technical requirements, generally based on experience, have been compiled by regulatory bodies. Deterministic criteria have been defined in such a way that it is very improbable that the load for which the bridge has been designed will be exceeded. Events considered to be probable must be completely controlled; those thought to be improbable are not considered explicitly.

If all the rules are applied correctly the bridge is safe. A collapse is very improbable, but it is not impossible. The remaining risks can be estimated from statistics about the collapse of similar bridges. Such an estimation requires expert judgement and is necessarily subjective. The safety of nuclear installations is also assured by the use of such deterministic criteria.

How to measure safety without statistics

Industrial activities result in the emission of about 20 billion tons of carbon dioxide per year, 100 million tons of sulphur, two million tons of lead, and so on. A large petro-chemical complex at Canvey Island, near London, has the capacity to store more than 100 000 tons of LNG and 10 000 tons of ammonia [3]. A nuclear reactor contains about 8 billion curies of radioactive substances.

All these activities pose a large potential threat to man and his environment. However, there is no clear statistical evidence of what causes climatic change, or of the relationship between certain pollutants and health or environment impact. There is also, fortunately, no statistical data base for nuclear or LNG accidents comparable to that for bridges.

Risks must be assessed for two main reasons.

- Systems have become so large and thus the potential consequences of accident so significant that we cannot

* Mr Niehaus is Head, Risk Assessment Section, in the Agency's Division of Nuclear Safety.

wait for statistical evidence to accumulate before errors are corrected; and

- Systems have become so complex that intuition and experience are no longer sufficient to enable designers to foresee all possible and significant events.

Thus, theoretical models, usually making use of sophisticated computer codes, must substitute for practical experience. Such models are based on available information about small components of the total system and on knowledge of chemical and physical phenomena. If the calculational codes incorporate all data and all interactions of system components, it is possible to simulate the behaviour of the total system.

Three short examples may serve to illustrate this approach.

1. As noted earlier, man's activities result in the emission of about 20 billion tons of CO_2 each year. Roughly half of this remains in the atmosphere and slowly but steadily changes its composition. CO_2 is fundamental to the existence of life: but how do we know that emissions on this scale are not causing irremediable damage to the environment? To answer this question a risk assessment is performed.

There is information about the solubility of the gas in salt water, isotope profiles in the oceans, rates of assimilation in plants, the growth of forests, atmospheric heat transfer, air circulation, the behaviour of ice cover, and so on. All this information must be incorporated into models which simulate the increase in atmospheric CO_2 as a result of different rates of consumption of fossil fuels and permit estimation of the climatic changes to be expected.

2. The second example relates to sulphur dioxide, SO_2, which is known to cause damage to health and the environment. Mankind's activities result in the emission of millions of tons of SO_2 per year, mainly from the burning of fossil fuels. Since a direct observation of the risks of such emissions is impossible, how do we know the potential consequences? To answer this question, atmospheric dispersion models are used to estimate ambient concentrations. Epidemiological studies are carried out to establish a dose-effect relationship. Population models then permit assessment of the total risk. As in the first example, there are large uncertainties. No definite answer is possible; only a probabilistic analysis can be made.

3. The first two examples related to routine industrial operations. The following example, however, has to do with hypothetical accidents. An operating nuclear power plant contains, as noted earlier, about $8 \cdot 10^9$ Ci of radioactive substances. A large storage tank can contain 20 000 tons of LNG. If a major fraction of such substances were released a catastrophe could occur. Statistical experience of large accidents is not available: how, therefore, do we know what precautions have to be taken?

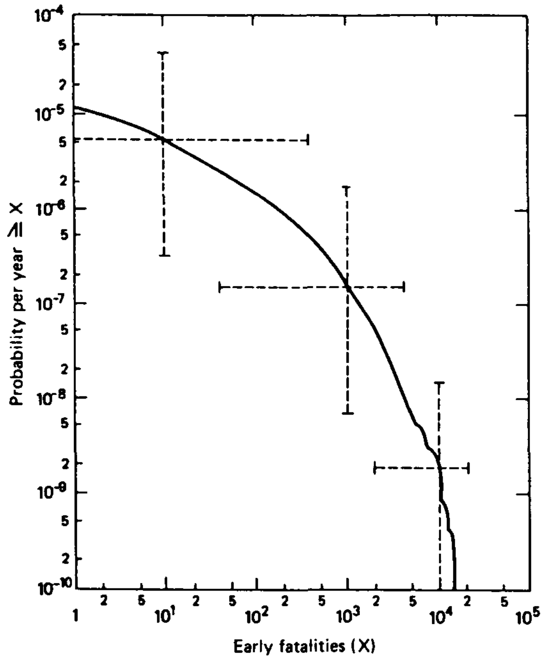

Figure 1. Results of risk assessment studies are usually displayed in the form of cumulative probability distributions. They show the probability that accidents occur which exceed a given number of fatalities, here for 25 plants in the Fed. Rep. of Germany [4]. The large dashed error bars indicate 90% subjective confidence that results are within the indicated bounds of probabilities or consequences.

As discussed earlier, safety precautions based on deterministic criteria have been taken to ensure the safety of such plants. However, some questions remain: what consequences are to be expected from "events" exceeding the design criteria, and what is their probability of occurrence? To answer such questions a Probabilistic Risk Analysis (PRA) can be performed. Accident sequences are modelled and potential releases and dispersion of substances are estimated. The combination of estimated exposures with population models then permits the calculation of potential consequences.

Limitations of risk assessment

Because of the lack of experience, such theoretical, computer modelling exercises are subject to large uncertainties with respect both to possible consequences and their probability of occurrence. Turning to the nuclear example, Figure 1 shows the cumulative probability distribution of early fatalities according to the "German Risk Study (DRS)* [4] which estimated

* Deutsche Risikostudie.

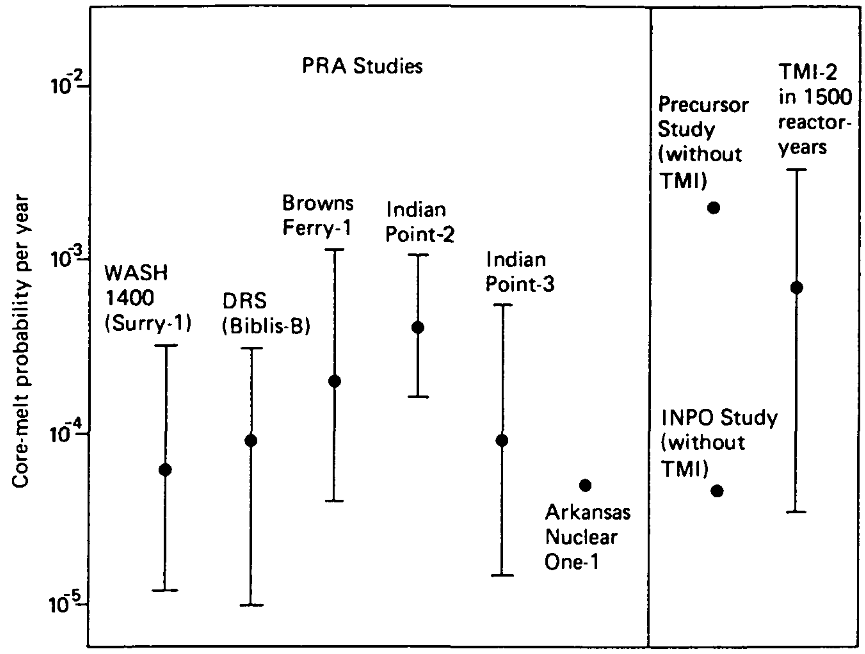

Figure 2. Estimates of probabilities for severe reactor core-melt according to different studies. Differences reflect as well difference in the design of plants. The most important contribution of risk assessment lies in the identification of important possible impacts or accident sequences and their causes (from Ref.[5]).

recently risks from nuclear reactors in the Fed. Rep. of Germany. The dashed bars indicate subjective 90% confidence intervals which extend over nearly three orders of magnitude. Even larger uncertainties must be considered if the results of different studies are compared. The left-hand side of Figure 2 is a compilation of the results of some PRA studies of core-melt frequency – which is to a large extent independent of site – including, where available, 90% confidence intervals. The right-hand side of the diagram shows results of the "Precursor Study" [2] and the "INPO** Study" [5]. The Three Mile Island accident, the only accident so far which resulted in a partial core-melt, is indicated. With one observed core-melt accident in 1500 reactor-years, the probability of a core-melt may be taken as about $7 \cdot 10^{-4}$ per reactor-year. This estimate is of course subject to a large uncertainty, as it is based on observation of only one such accident.

In reality, the uncertainties are much larger. The main reasons for this lie in:

- limitations of the studies themselves (usually not all risks are considered – e.g. unplanned human intervention in the case of nuclear plants, other trace substances in the CO_2 case and synergistic effects of other pollutants in the SO_2 case);
- limitations of the analysis, especially with regard to common-mode failure and human error (only those accidents which have been anticipated can be analysed); and
- limitations in available data (usually displayed in the results).

** Institute of Nuclear Power Operations.

Application of the results of risk assessments

Given the large uncertainties, it must be asked what use can be made of such analyses. Of course, the answer is not identical for the various types of risk assessment study. However, the following four main areas of application emerge.

1. The most important application of risk assessment studies is in the identification of major contributors to risk: important possible impacts or accident sequences and their causes can be identified, together with effective means of controlling them. The German Risk Study identified about 40 possible design changes which would effectively reduce risk [4]. It was also possible to demonstrate the important rôle of human failure in ensuring safety (Fig.3). An example from the non-nuclear field is given in Figure 4 [3]. It was possible to improve the safety of the Canvey Island complex significantly after a risk analysis had been made. Risk assessments can also be used to evaluate and compare different designs or sites for proposed facilities, all of which would meet established safety requirements.

2. Risk assessment can be used to develop further those deterministic criteria which at present ensure the safety of technical installations.

3. If the uncertainties are reasonably low, the results of risk assessment studies can be used to put certain risks into perspective.

4. If the uncertainties in the absolute numbers are very large, the process of performing the analysis might be more important in itself than the results obtained. Systematic modelling improves understanding of the

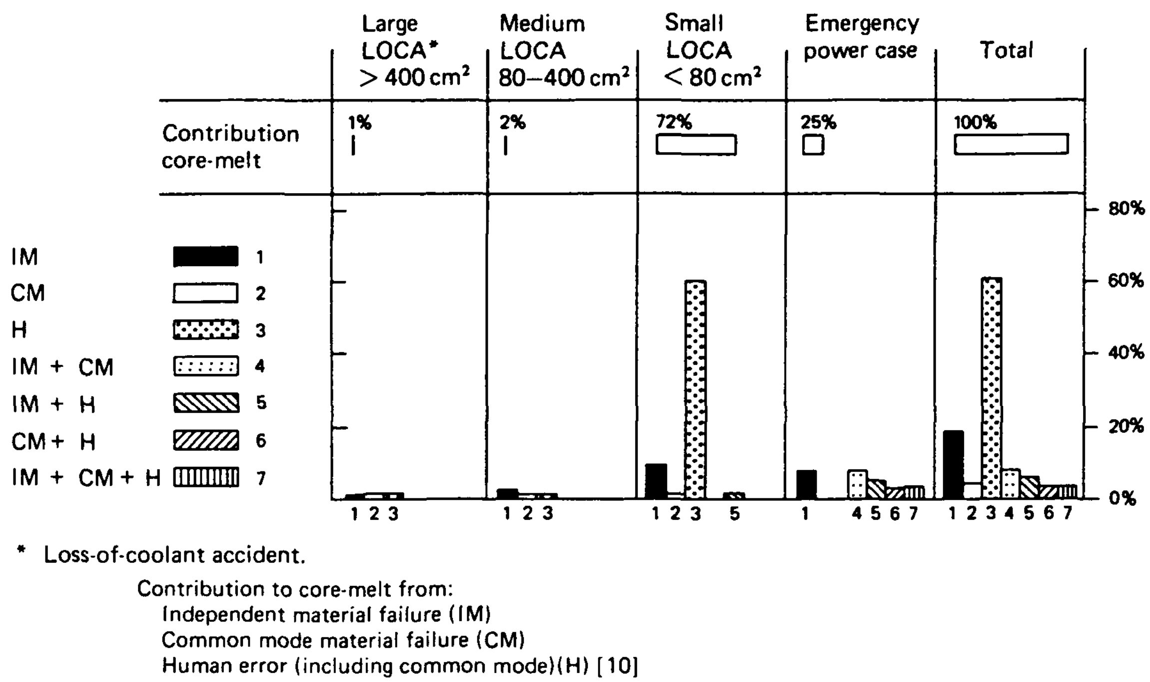

Figure 3. This bar chart indicates that more than 60% of all estimated core-melt accidents would be caused by human failure (from Ref.[4]).

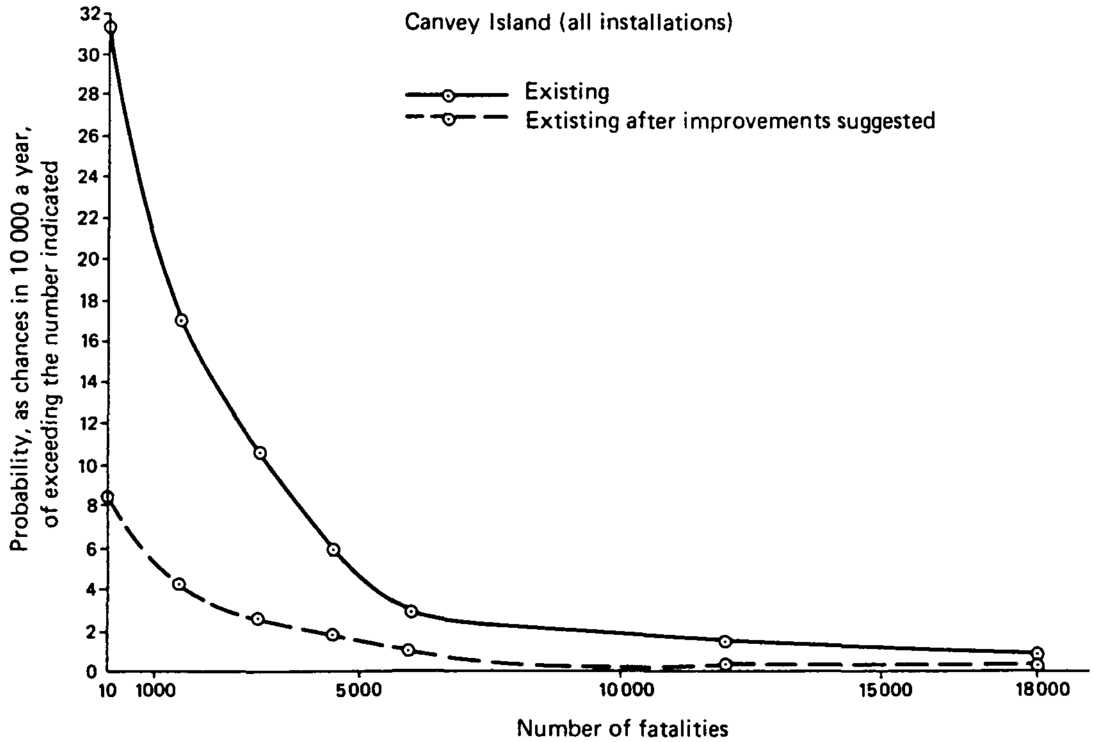

Figure 4. Following a risk assessment study for Canvey Island, a large petro-chemical complex, a certain number of improvements have been suggested which are very effective in reducing risk (from Ref.[3]).

interaction of system components. Often, qualitative conclusions are sufficient in themselves to guide improvements in safety.

Qualitative differences

So far, only technical data and methodological aspects have been discussed. However, in spite of the fact that two different risks might on average harm the same number of people, one might want to spend more effort to reduce one of them because of its physical properties or because it is more frightening. A collection of factors known to influence the significance of risks is given in Table 1 [6]. Two examples will be described to highlight briefly this problem area, which is usually termed "risk evaluation".

Table 1. Risks can be qualitatively different, even if on average or in the long-term they cause the same damage. This applies to different types of health effect as well as to who is exposed and how. This table summarizes some of these factors

• Occupational	–	Public effects
• Individual	–	Population exposure
• Voluntary	–	Involuntary exposure
• Immediate	–	Delayed effects
• Controllable	–	Uncontrollable effects
• High probability/low consequence (HP/LC)	–	Low probability/high consequence (LP/HC)
• Low uncertainty	–	High uncertainty

Low Probability/High Consequence Risks: Much concern is expressed about accidents which involve a large number of people at the same time. Should accidents affecting one person per year be treated identically to accidents occurring once in a thousand years but affecting 1000 people? It is a general tendency of modern technologies that increased safety results in a qualitative shift from high probability/low consequence to low probability/high consequence risk. An example of this (coupled with technical and economic considerations) lies in aircraft accidents, as shown in Figure 5 [7]. The average risk per passenger·kilometer has fallen significantly. However,

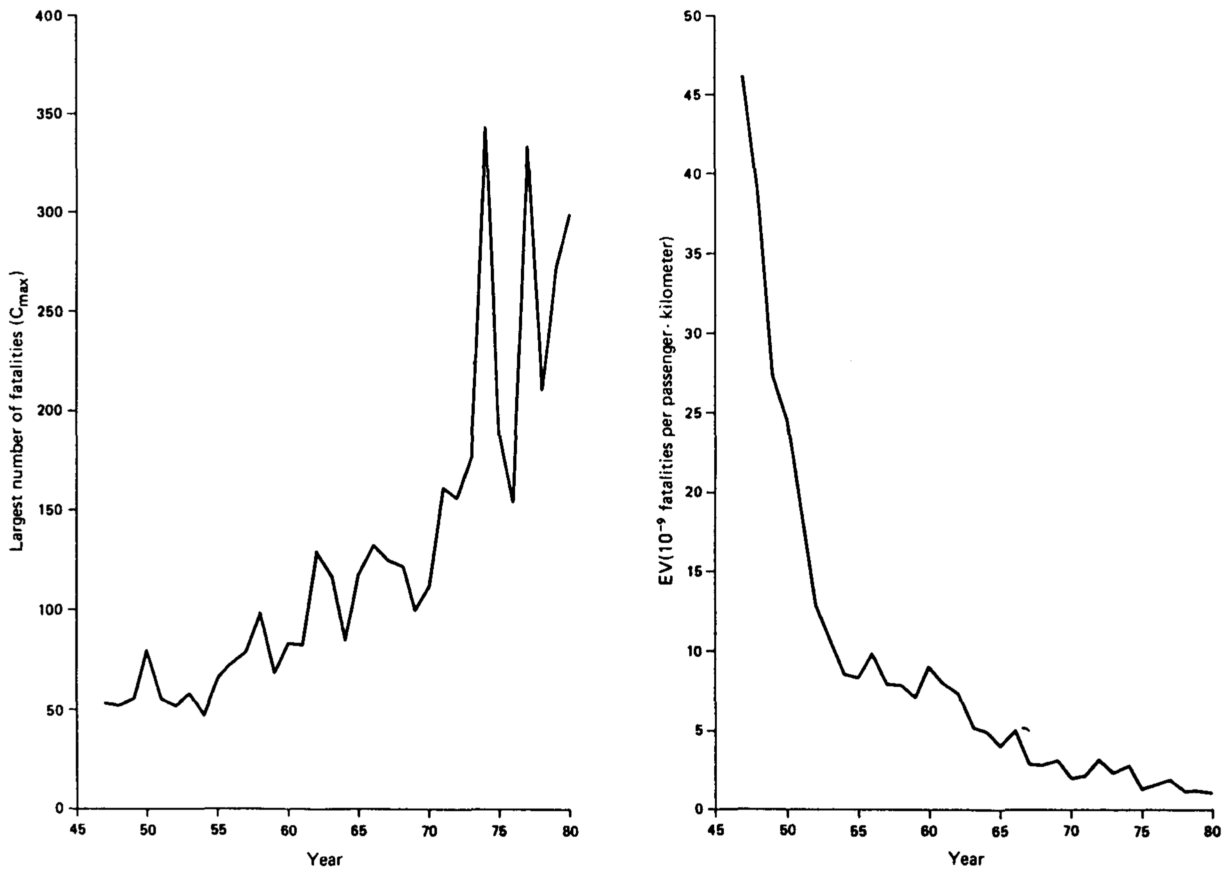

Figure 5 a + b. The diagrams show the historical development of aircraft accidents. The improvements in reducing the average risk per passenger kilometer (EV) had to be paid for by increasing the chance of accidents involving more people at the same time. The largest accident in a given year (one aircraft only) has been plotted as C_{max}. It is evident that a qualitative shift in risk, driven by many different causes, occurred. The same phenomenon can be seen in many other modern technologies. (Note change of scale.)

this achievement has had to be paid for by increasing the potential for low probability/high consequence accidents involving many passengers at the same time.

Uncertainties in risks: All assessments of risk are subject to uncertainties. Uncertainty about a possible outcome is one of the most important attributes of a "risky" situation. An example may illustrate this. Using design "A" it is known precisely that this technology could lead to accidents which once in a thousand years would affect 100 people. Thus, on average, one death might be expected every 10 years. The best estimate for alternative design "B" is on average exactly the same. However, it is not known whether only 10 but in the worst case also 1000 people might be affected. Choosing between the two designs, most people would definitely prefer design "A" since it reduces uncertainties. Thus, uncertainty is one of the most important aspects of a risky situation (see also [8]).

Decision criteria

As we have seen, safety is ensured by observance of mainly deterministic criteria which are to a large extent based on experience, gained either directly or by extrapolation from other experience. As a supplement to the use of such criteria some countries are developing qualitative and quantitative safety goals. An example is given by the preliminary quantitative design objectives recently published by the US NRC for use during a two-year evaluation period, which are summarized in Table 2 [2]. Safety goals can be based on the following general criteria:

1. A goal can be set to limit individual risk in the vicinity of the plant. This can be based on an average person or on the individual exposed to the highest risk.
2. In addition, a goal can be set to limit societal risk or risk to population sub-groups.
3. These two goals can be supplemented by an efficacy criterion: to reduce risks even further if this can be achieved at a certain cost, or if it is technical achievable, or if it is practical, and so on.
4. In addition, certain limits can be set for the probability or consequences of certain types of accident (e.g. core-melt) or the performance of certain safety systems (e.g. containment).

A whole set of such criteria can be developed or certain criteria can be singled out. Consideration can also be given to certain qualitatively different types of risk as discussed above. It is, for example, possible to put additional constraints on large accidents [9] or to develop different criteria for routine operation or possible accidents [10]. However, it has to be stressed that the usefulness of risk assessment is not subject to the establishment of safety goals or design objectives.

So far, there is limited experience with quantitative safety goals. Considering the uncertainties inherent in risk assessment, it will be necessary to forge a strong link between the goals and the method of assessment and to define precisely under what conditions it has been proven that certain goals have been met. In any case, risk assessment, possibly supplemented by safety goals, will in future be used to develop further the present deterministic safety criteria and reliability of system components.

Table 2. The US NRC has decided to adopt qualitative safety goals supported by quantitative design objectives for nuclear plants for use during a two-year evaluation period. The quantitative objectives are summarized in this table

US Nuclear Regulatory Commission Quantitative Design Objectives

- *Individual risk:* The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one per cent of the sum of prompt fatality risks resulting from other accidents to which members of the US population are generally exposed.
- *Societal risks:* The risk to the population in the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one per cent of the sum of cancer fatality risks resulting from all other causes.
- *Efficacy:* The benefit of an incremental reduction of societal mortality risks should be compared with the associated costs on the basis of US $1000 per person-rem averted.
- *Core performance:* The likelihood of a nuclear reactor accident that results in a large-scale core melt should normally be less than one in 10 000 per year of reactor operation.

Public acceptance

The main purpose of risk assessment is to improve safety and minimize risk, and not to gain public acceptance for certain technologies. However, quantitative technical data can have an important rôle in rationalizing discussion or controversy. In such a process, the absolute numbers are less important than the general perspective given by the results. Risk assessment can also help to draw attention to the relative significance of a problem. In the case of nuclear power, for example, it seems to be necessary not to lose sight of the important fact that nuclear power has a very low environmental impact during routine operation [11]. In addition to the advantage of helping to put problems or partial problems into perspective, risk assessment will help improve trust in regulatory institutions by making regulations more consistent and transparent. A gain in the credibility of, and trust in, regulatory institutions will be the most important contribution of risk assessment in increasing the public's acceptance of nuclear power.

Highlights of IAEA Risk Assessment Programme

The *International Symposium on the Risks and Benefits of Energy Systems,* to be held at the Nuclear Research Centre, Jülich, FRG, 9–13 April 1984, has the objective to analyse the rôle of nuclear power in perspective with other energy supply systems, and to give a balanced account of both the risks and benefits involved.

The IAEA co-ordinated research programme (15 Member States participating) on *Comparison of Cost-Effectiveness of Risk Reduction Among Different Energy Systems* has the objective to determine optimal allocation of resources for increasing safety in the total fuel cycle of energy systems [12].

The IAEA co-ordinated research programme (15 Member States participating) on *Development of Risk Criteria for the Nuclear Fuel Cycle* has the objective to develop a consistent set of methods and criteria for the expression of risks for the total light-water reactor fuel cycle [13].

An IAEA programme consisting of seminars, courses, expert meetings, and technical documents on specific subjects has the objective to collect, assess, and disseminate information on the methods and results of risk assessment work in Member States, including public understanding of nuclear safety.

Conclusions

In spite of the large uncertainties, risk assessment will in the future play a rapidly growing rôle in ensuring the safety of large-scale industrial installations, including those of the nuclear fuel cycle. Important insights can be derived from quantitative risk assessments, especially in identifying important parameters of risk. Even if the uncertainties are large, the insights gained from the process of performing the analysis will be helpful in improving safety.

The thorough understanding of systems provided by risk assessment is at least useful for:

- evaluating safety by improved training of staff;
- determining research and development priorities;
- further developing deterministic safety criteria; and
- complementing present-day safety by treating the interactions of the total system including (improbable) events which can be derived theoretically only.

Thus, risk assessment is designed not to replace the current approach to ensuring safety, but to complement it; and it will help to improve deterministic safety criteria. It has the potential as well to enhance the credibility of regulatory bodies by making regulations more consistent and transparent. If the limits of risk assessment are understood properly, it can serve as an important tool to ensure nuclear safety in coming decades.

References

[1] **H. Inhaber, S. Norman,** *The Increase in Risk Interest. Risk Analysis* Vol.2, No.3 (1982).

[2] **US Nuclear Regulatory Commission** *Policy Statement on Safety Goals for the Operation of Nuclear Power Plants* No. 83–39, Office of Public Affairs, Washington, D.C. 20555 (14 March 1983).

[3] **Canvey Island Study,** *Canvey: Summary of an Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area* Health and Safety Executive, London (1978).

[4] **Deutsche Risikostudie, Kernkraftwerke:** *Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko* TUeV Rheinland GmbH, Köln (1979).

[5] **A. Birkhofer,** *Das Risikokonzept aus naturwissenschaftlich-technischer Sicht* Kurzreferat beim 7. Deutschen Atomrechts-Symposium 1983, Göttingen (FRG) (16 March 1983).

[6] **F. Niehaus, E. Swaton,** *Risk Assessment and Public Acceptance of Nuclear Power* Serie Seminari, ENEA, Rome, Italy (1981).

[7] **F. Niehaus, G. de Leon, M. Cullingford,** *The Trade-Off between Expected Risk and the Potential for Large Accidents* Presented at the Workshop on Low Probability/High Consequence Risk Analysis, 15–17 June 1982, Arlington, Virginia, USA.

[8] **P. Slovic, B. Fischhoff, S. Lichtenstein,** *Is Society Really Risk Adverse?* Presented at the Workshop on Low probability/High consequence Risk Analysis, 15–17 June 1982, Arlington, Virginia, USA.

[9] **US Nuclear Regulatory Commission** *An Approach to Quantitative Safety Goals for Nuclear Power Plants* NUREG-0739 (1980).

[10] **M.J. Clark, A.B. Fleischman, G.A.M. Webb,** *Optimization of the Radiological Protection of the Public* NRPB-R120 (July 1981).

[11] **E. Swaton,** *Attitudes Toward Risk: A Cross-Cultural Comparison* Presented at the Status Seminar "Task, Methods and Predictive Power of Risk Research", 24–25 November 1980, organized by the University of Bielefeld, Bielefeld.

[12] **F. Niehaus, A. Novegno,** *Optimal Allocation of Resources for Safety* Presented at the Symposium on the Assessment and Perception of Risk To Human Health, 18–19 October 1982, Ontario, Canada.

[13] **M. Cullingford, F. Niehaus, S. Vuori,** *Use of Risk Analysis in Safety Decisions* Presented at the Annual Congress of the French Society of Radioprotection, 18–22 October 1982, Avignon, France.